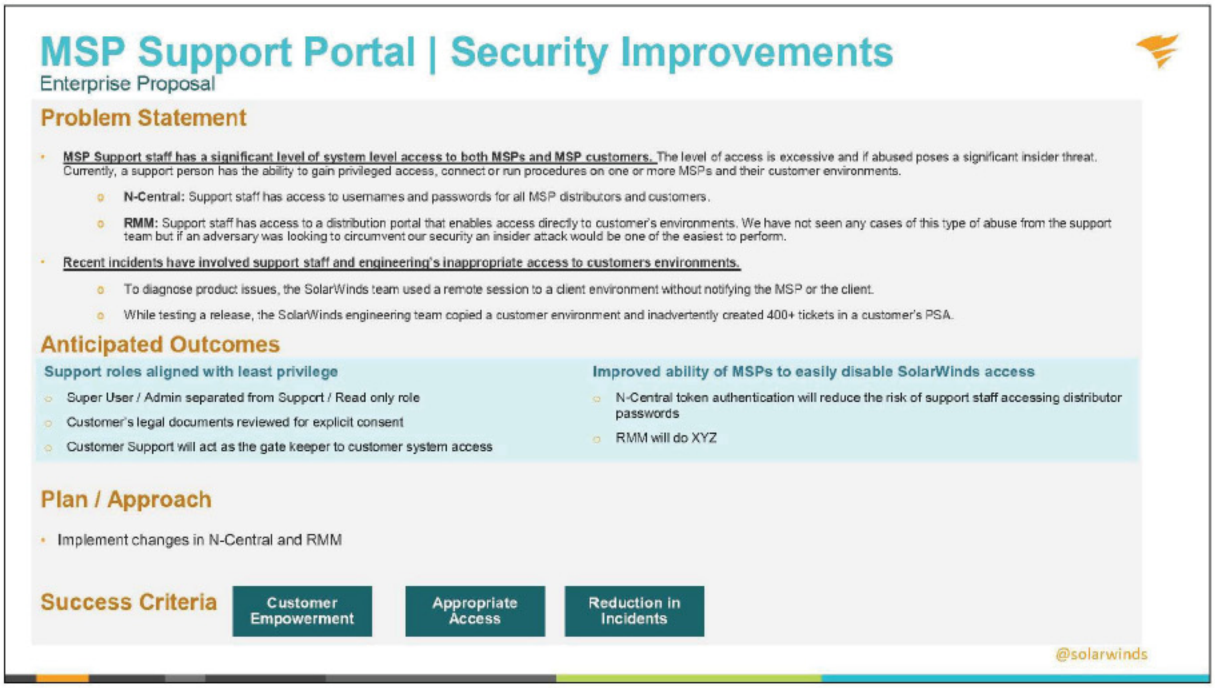
EXHIBIT 32

solarwinds

MSP Support Security Improvement

SECURITY

NOVEMBER 2019



MSP Support Portal | Security Improvements

Enterprise Proposal

Problem Statement

- **MSP Support staff has a significant level of system level access to both MSPs and MSP customers.** The level of access is excessive and if abused poses a significant insider threat. Currently, a support person has the ability to gain privileged access, connect or run procedures on one or more MSPs and their customer environments.
  - **N-Central:** Support staff has access to usernames and passwords for all MSP distributors and customers.
  - **RMM:** Support staff has access to a distribution portal that enables access directly to customer's environments. We have not seen any cases of this type of abuse from the support team but if an adversary was looking to circumvent our security an insider attack would be one of the easiest to perform.
- **Recent incidents have involved support staff and engineering's inappropriate access to customers environments.**
  - To diagnose product issues, the SolarWinds team used a remote session to a client environment without notifying the MSP or the client.
  - While testing a release, the SolarWinds engineering team copied a customer environment and inadvertently created 400+ tickets in a customer's PSA.

Anticipated Outcomes

Support roles aligned with least privilege

- Super User / Admin separated from Support / Read only role
- Customer's legal documents reviewed for explicit consent
- Customer Support will act as the gate keeper to customer system access

Improved ability of MSPs to easily disable SolarWinds access

- N-Central token authentication will reduce the risk of support staff accessing distributor passwords
- RMM will do XYZ

Plan / Approach

- Implement changes in N-Central and RMM

Success Criteria

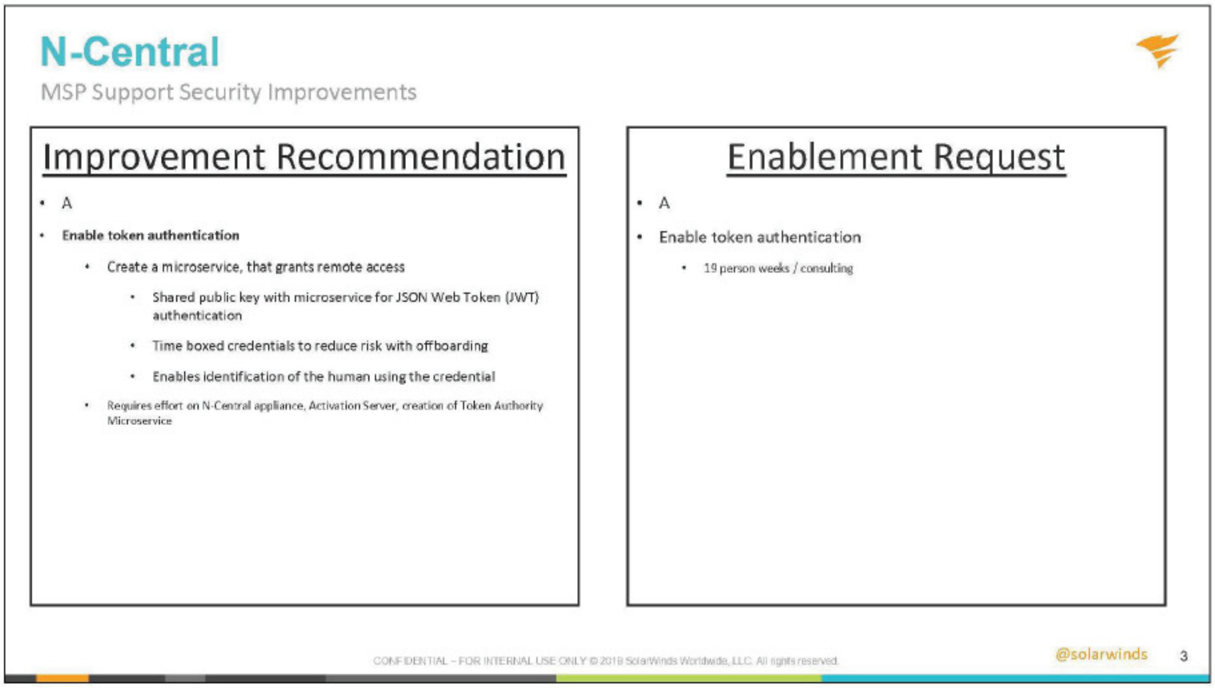
Customer Empowerment

Appropriate Access

Reduction in Incidents

@solarwinds

What is PSA?



N-Central

MSP Support Security Improvements

Improvement Recommendation

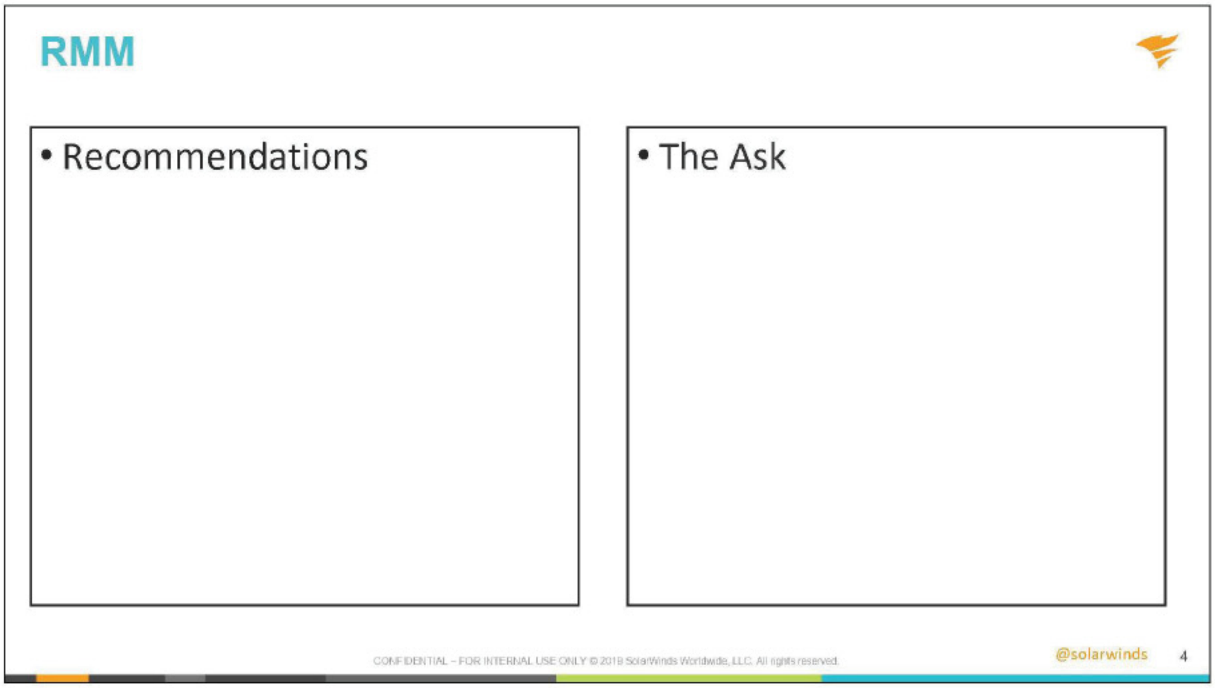
- A
- **Enable token authentication**
  - Create a microservice, that grants remote access
    - Shared public key with microservice for JSON Web Token (JWT) authentication
    - Time boxed credentials to reduce risk with offboarding
    - Enables identification of the human using the credential
  - Requires effort on N-Central appliance, Activation Server, creation of Token Authority Microservice

Enablement Request

- A
- Enable token authentication
  - 19 person weeks / consulting

CONFIDENTIAL – FOR INTERNAL USE ONLY © 2019 SolarWinds Worldwide, LLC. All rights reserved.

@solarwinds 3

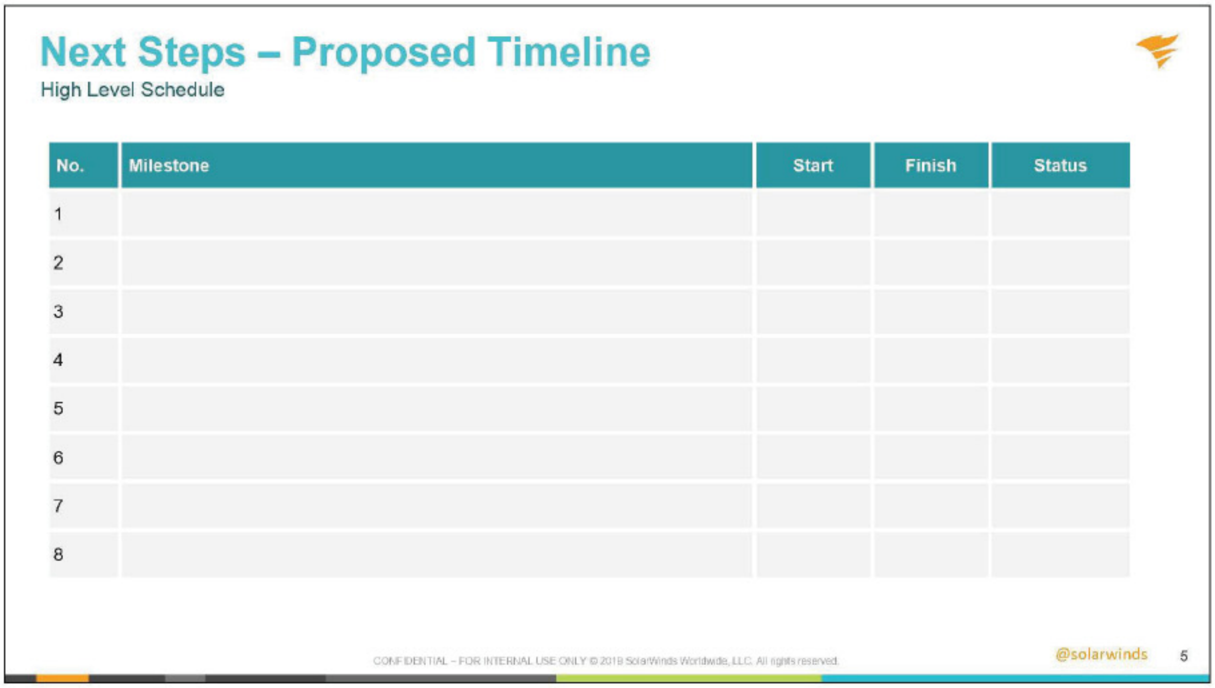


RMM

- Recommendations

- The Ask

@solarwinds



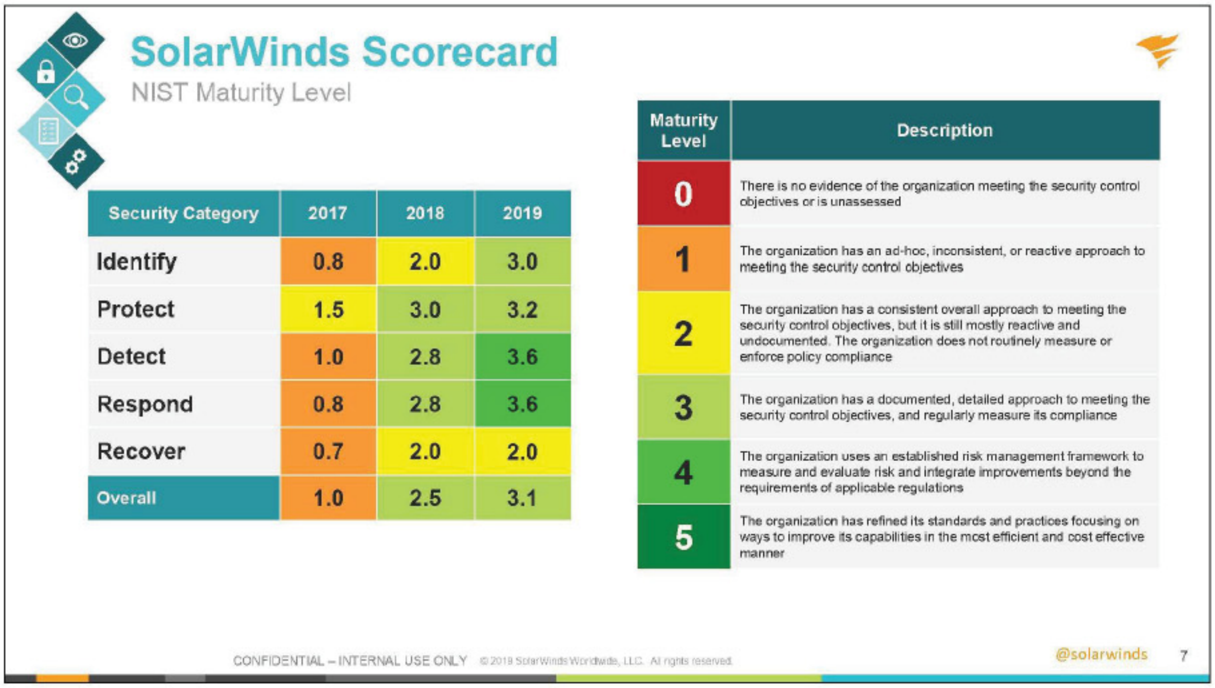
Next Steps – Proposed Timeline

High Level Schedule

No.	Milestone	Start	Finish	Status
1				
2				
3				
4				
5				
6				
7				
8				

THANK YOU!

@solarwinds



SolarWinds Scorecard

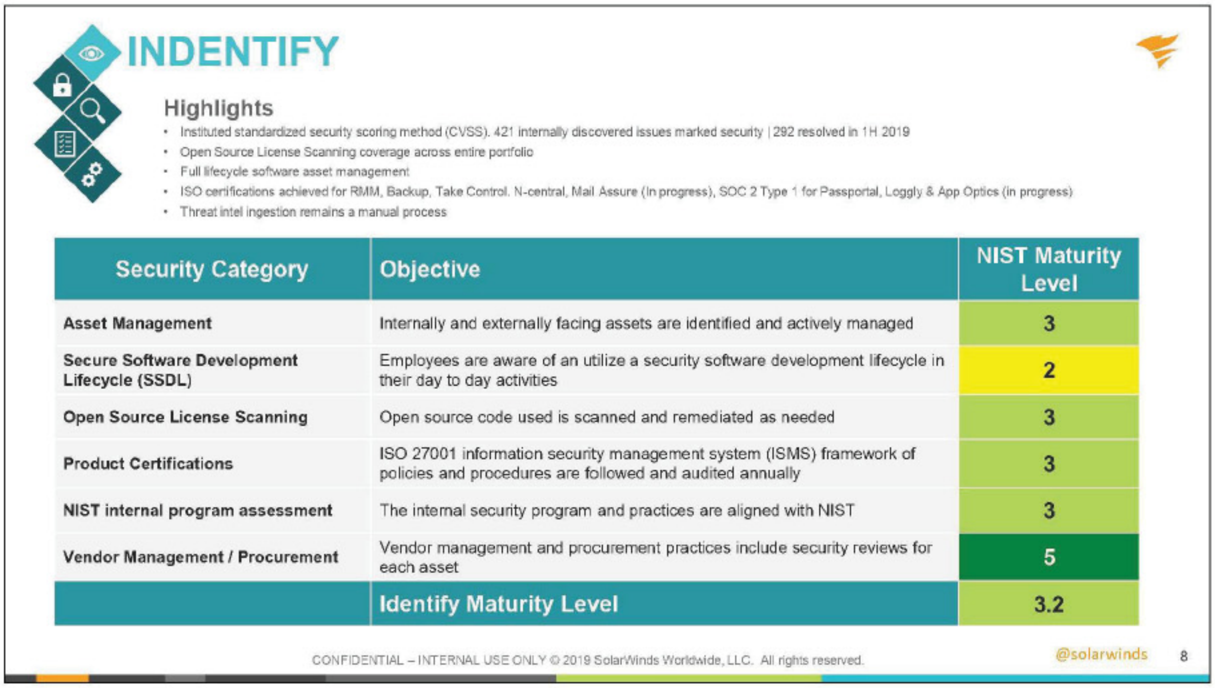
NIST Maturity Level

Security Category	2017	2018	2019
Identify	0.8	2.0	3.0
Protect	1.5	3.0	3.2
Detect	1.0	2.8	3.6
Respond	0.8	2.8	3.6
Recover	0.7	2.0	2.0
Overall	1.0	2.5	3.1

Maturity Level	Description
0	There is no evidence of the organization meeting the security control objectives or is unassessed
1	The organization has an ad-hoc, inconsistent, or reactive approach to meeting the security control objectives
2	The organization has a consistent overall approach to meeting the security control objectives, but it is still mostly reactive and undocumented. The organization does not routinely measure or enforce policy compliance
3	The organization has a documented, detailed approach to meeting the security control objectives, and regularly measure its compliance
4	The organization uses an established risk management framework to measure and evaluate risk and integrate improvements beyond the requirements of applicable regulations
5	The organization has refined its standards and practices focusing on ways to improve its capabilities in the most efficient and cost effective manner

CONFIDENTIAL – INTERNAL USE ONLY

@solarwinds 7



INDENTIFY

Highlights

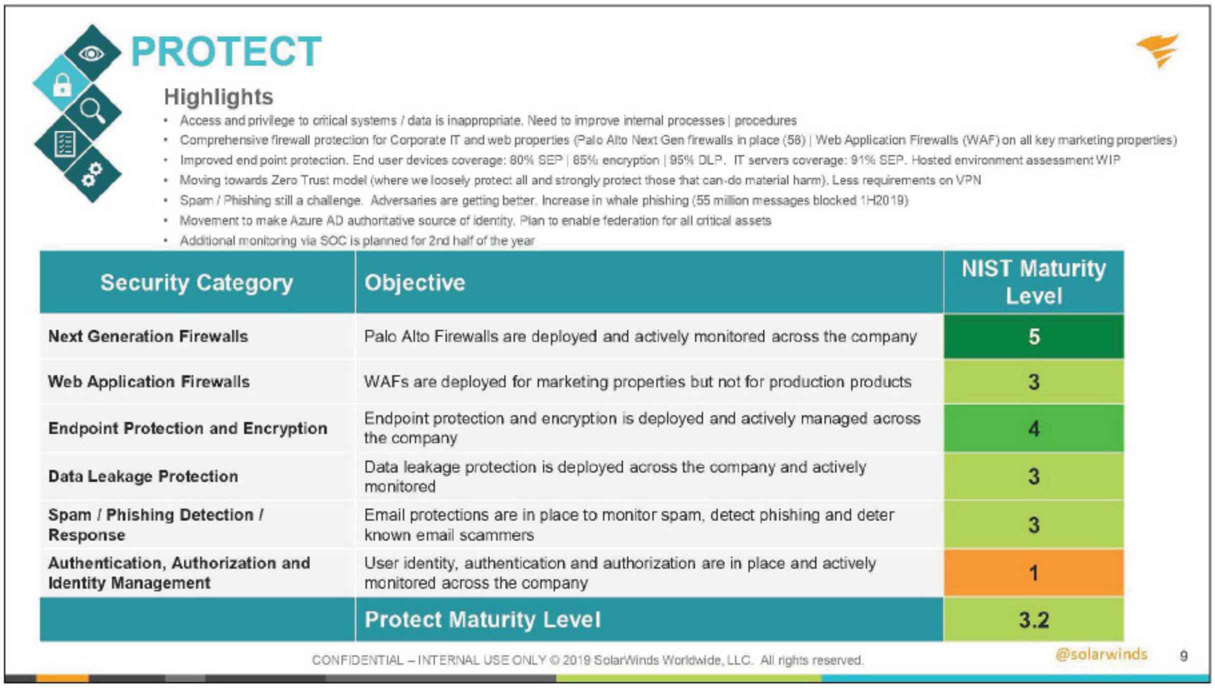
- Instituted standardized security scoring method (CVSS). 421 internally discovered issues marked security | 292 resolved in 1H 2019
- Open Source License Scanning coverage across entire portfolio
- Full lifecycle software asset management
- ISO certifications achieved for RMM, Backup, Take Control. N-central, Mail Assure (In progress), SOC 2 Type 1 for Passportal, Loggly & App Optics (in progress)
- Threat intel ingestion remains a manual process

Security Category	Objective	NIST Maturity Level
Asset Management	Internally and externally facing assets are identified and actively managed	3
Secure Software Development Lifecycle (SSDL)	Employees are aware of an utilize a security software development lifecycle in their day to day activities	2
Open Source License Scanning	Open source code used is scanned and remediated as needed	3
Product Certifications	ISO 27001 information security management system (ISMS) framework of policies and procedures are followed and audited annually	3
NIST internal program assessment	The internal security program and practices are aligned with NIST	3
Vendor Management / Procurement	Vendor management and procurement practices include security reviews for each asset	5
	Identify Maturity Level	**3.2**

CONFIDENTIAL – INTERNAL USE ONLY © 2019 SolarWinds Worldwide, LLC. All rights reserved.

@solarwinds 8

495/6 =82.5



PROTECT

Highlights

- Access and privilege to critical systems / data is inappropriate. Need to improve internal processes | procedures
- Comprehensive firewall protection for Corporate IT and web properties (Palo Alto Next Gen firewalls in place (56) | Web Application Firewalls (WAF) on all key marketing properties)
- Improved end point protection. End user devices coverage: 80% SEP | 85% encryption | 95% DLP. IT servers coverage: 91% SEP. Hosted environment assessment WIP
- Moving towards Zero Trust model (where we loosely protect all and strongly protect those that can-do material harm). Less requirements on VPN
- Spam / Phishing still a challenge. Adversaries are getting better. Increase in whale phishing (55 million messages blocked 1H2019)
- Movement to make Azure AD authoritative source of identity. Plan to enable federation for all critical assets
- Additional monitoring via SOC is planned for 2nd half of the year

Security Category	Objective	NIST Maturity Level
Next Generation Firewalls	Palo Alto Firewalls are deployed and actively monitored across the company	5
Web Application Firewalls	WAFs are deployed for marketing properties but not for production products	3
Endpoint Protection and Encryption	Endpoint protection and encryption is deployed and actively managed across the company	4
Data Leakage Protection	Data leakage protection is deployed across the company and actively monitored	3
Spam / Phishing Detection / Response	Email protections are in place to monitor spam, detect phishing and deter known email scammers	3
Authentication, Authorization and Identity Management	User identity, authentication and authorization are in place and actively monitored across the company	1
	Protect Maturity Level	3.2

CONFIDENTIAL – INTERNAL USE ONLY © 2019 SolarWinds Worldwide, LLC. All rights reserved. @solarwinds 9

399/5=79.8

Q&A

@solarwinds